Office of the Governor
State Chief Information Officer

SECURITY

Chapter 4 – Purchasing and Maintaining Commercial Software

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: N.C.G.S. 147-33.110

Section 01 Purchasing and Installing Software

040101 Specifying User Requirements for Software

Purpose: To require business justifications for applications software purchases/enhancements.

STANDARD

Agencies shall ensure that a business justification accompanies all requests for new application systems or software enhancements. The justification shall include the following:

- Documented business needs and expectations of the new system or enhancement.
- Preliminary risk assessment and cost analysis identifying the business value of the assets involved, the security requirements for the system and the compatibility with other system parts.
- Statement of senior management approval, prior to procurement.

GUIDELINES

Each agency should have a formal business justification procedure to identify business, security and technical requirements that new systems and software enhancements should meet. Using a well-defined process explores technical, security and business issues and helps the agency avoid:

- Security risks arising from inadequate security controls.
- Failing to meet business needs and expectations by choosing less than the best solution.
- Unexpected cost and wasted time retrofitting an inadequate solution.

ISO 17799: 2005 REFERENCE
6.1.4 Authorization process for information processing facilities

040102 Selecting Business Software Packages

Purpose: To protect agency resources during the software selection process.

STANDARD

Agencies shall ensure that a formal selection process is used to purchase business-critical software necessary to deliver public services such as accounting, general ledger, and inventory control. The selection process shall include a review of security measures needed to protect the confidentiality, availability and integrity of the data.

GUIDELINES

Agencies should minimize the likelihood of selecting poorly designed or inadequate software by taking the following steps:

- Avoiding software that fails to meet business needs.
- Avoiding software for which support is not readily available.
- Reviewing proprietary software used in a production environment annually to assess the exposure from using old or outdated programming languages, databases and protocols.
- Ensuring that software under consideration for purchase works with the majority of peripherals and systems currently in use.
- Avoiding software packages that have been highly customized.

RELATED INFORMATION

Standard 040205 Supporting Application Software

ISO 17799: 2005 REFERENCE
6.1.4 Authorization process for information processing facilities

040103 Selecting Office Software Packages

Purpose: To increase interoperability by standardizing software packages.

STANDARD

Agencies shall ensure the following:

- That office software packages installed on agency computers comply with the agency's security requirements.
- That management-approved criteria for the selection of software packages are defined and documented.
- That software under consideration for acquisition works with the majority of peripherals and systems currently in use.

GUIDELINES

When selecting office software packages, agencies should consider that:

- Old or outdated software typically poses a higher security risk than updated office software.
- The standard office software package is more effective when universally used across State agencies to ensure compatibility among divisions and agencies.
- Upgrading office automation software may necessitate the purchase of new hardware.

ISO 17799: 2005 REFERENCE
12.1.1 Security requirements analysis and specification

040104 Using Licensed Software

Purpose: To require compliance with software licensing agreements.

STANDARD

Agencies shall ensure that all software is licensed and that users adhere to the terms of the end user license agreement. Such adherence is necessary to comply with legislation and to ensure continued vendor support, including vendor provision of patches and updates that address security flaws.

ISO 17799: 2005 REFERENCE
15.1.2 Intellectual property rights (IPR)

040105 Implementing New / Upgraded Software

Purpose: To control security risks involved when implementing new or upgraded software.

STANDARD

Agencies shall design security into systems used for data processing so that the systems have the proper technical and procedural security controls.

GUIDELINES

New or upgraded software should not be made available to users until a risk analysis (RA) and/or business impact analysis (BIA) is performed and the risks are understood.

In conjunction with the RA and/or BIA, agencies should develop the following:

- A step-by-step implementation plan.
- A software implementation plan that follows change control procedures.
- Management and user acceptance criteria, including:
  - Desired acceptance tests and their desired results.
  - Demonstration that computer capacity and performance requirements are not adversely affected.
  - Assurance that system security controls will remain effective.
  - Amendments to system documentation and business continuity plans to reflect the software implemented.

- A rollback plan for use in the event the implementation has unacceptable ramifications.

Agencies should also consider the potential impact software upgrades may have on the following:

- Interdependent systems that rely on some functionality of the upgraded system.
- Overall information security throughout the agency's environment.
- Training needs for business and technical users covering new features and security controls introduced by the upgrade.

RELATED INFORMATION

Standard 140102 Assessing the Business Continuity Plan Security Risk

ISO 17799: 2005 REFERENCE
12.5.1 Change control procedures

040106 Technical Vulnerability Management

Purpose: To establish requirements for an ongoing program of vulnerability mitigation that includes information review and analysis, as well as metrics tracking and reporting.

STANDARD

Vulnerabilities that threaten the security of the state's network shall be addressed through updates and patches based upon assigned vulnerability ratings.

2.1 Vulnerability Risk Ratings

The risk ratings assigned to a vulnerability are:

- *High-level Risk:* A vulnerability that could cause grave consequences if not addressed and remedied immediately. This type of vulnerability is present within the most sensitive portions of the network, as identified by the data owner. This vulnerability could cause network functionality to cease or control of the network to be gained by an intruder.

- *Medium-level Risk:* A vulnerability that should be addressed within the near future. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner.

- *Low-level Risk:* A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network to be exploited and/or it is of little consequence to the data owner. Vulnerabilities of this nature are common among most networks and usually involve a simple patch to remedy the problem. These patches can also be defined as enhancements to the network.

Vulnerability Mitigation

1. Mitigation timeframes for identified or assessed vulnerabilities shall be based on the assigned Vulnerability Risk Rating:

2. "High-level risk" vulnerabilities must be mitigated within seven (7) days.

3. "Medium-level risk" vulnerabilities must be mitigated within thirty (30) days.

4. "Low-level risk" vulnerabilities must be mitigated within ninety (90) days.

5. Agency vulnerability mitigation plans must specify, at a minimum, the proposed resolution to address identified vulnerabilities, required tasks necessary to affect changes, and the assignment of the required tasks to appropriate personnel.

6. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available. When a vulnerability risk is 'high-level' and no patch is available steps must be taken to mitigate the risk through other methods (*e.g.*, workarounds, firewalls, and router access control lists). The patch needs to be applied when it becomes available. When a high-level risk vulnerability cannot be totally mitigated within the requisite time frame, agencies need to have procedures in place to notify agency management and the State Chief Information Officer of the existing condition.

7. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.

8. Appropriate notification shall be provided after vulnerability mitigation plans have been executed.

Vulnerability Information Review and Analysis

1. Relevant vulnerability information from appropriate vendors, third party research, and public domain resources should be reviewed on a daily basis.

2. Relevant vulnerability information, as discovered, shall be distributed to the appropriate agency employees, including but not limited to Information Security, Information Technology, and Internal Audit.

3. Appropriate agency personnel shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

Vulnerability Metrics Tracking and Reporting

1. The following vulnerability task assignment metrics must be routinely tracked for specific administrators and vendor technologies:
2. Number of new vulnerability task assignments
3. Number of closed vulnerability task assignments
4. Number of overdue vulnerability task assignments

5. Agency managers, including but not limited to Information Security, Information Technology, and Internal Audit, shall be provided with a quarterly report on the following vulnerability metrics:

    - Number of total vulnerabilities for the current quarter including those open at the beginning of the quarter
    - Number of vulnerabilities closed for the current quarter
    - Number of vulnerabilities open for the current quarter
    - Number of vulnerability exceptions for the current quarter
    - Severity level of vulnerabilities
    - Previous quarter vulnerability metrics

6. Vulnerability metrics and mitigation plans shall be retained for a minimum of two (2) years or as prescribed by legal or regulatory requirements.

Requirements for Compliance

1. Agencies must develop procedures to ensure the timely and consistent use of security patches and use a consistent vulnerability naming scheme to mitigate the impact of vulnerabilities in computer systems. Agencies shall have an explicit and documented patching and vulnerability policy, as well as a systematic, accountable, and documented set of processes and procedures for handling patches. The patching and vulnerability policy shall specify what techniques an organization will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring. An organization's patching process shall define a method for deciding which systems get patched and which patches get installed first. It shall also include a methodology for testing and safely installing patches.

2. An agency process for handling patches shall include:
    - Using organizational inventories
    - Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring[1]
    - Patch prioritization techniques
    - Organizational patch databases
    - Patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications.

3. Develop and maintain a list of sources of information about security problems and software updates for the system and application software.

4. Establish a procedure for monitoring those information sources.

5. Evaluate updates for applicability to the systems

6. Plan the installation of applicable updates

7. Install updates using a documented plan

8. Deploy new computers with up-to-date software.

[1] *See,* http://cve.mitre.org

9. After making any changes in a computer's configuration or its information content, create new cryptographic checksums or other integrity-checking baseline information for that computer.

ISO 17799: 2005 REFERENCE
12.6.1 Control of technical vulnerabilities

Section 02 Software Maintenance and Upgrade

040201 Applying Patches to Software

Purpose: To protect from risks associated with software patches.

STANDARD

Agencies shall develop procedures to ensure the timely and consistent use of security patches. A consistent vulnerability-naming scheme to mitigate the impact of vulnerabilities in computer systems must be used across the agency and State.

Agencies shall ensure that:

- Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources.
- The patch application process follows formal change control procedures that include the following controls prior to installation:
  - Verification of the source of the patch.
  - Verification of the need for the patch.
  - Testing of the patch.
  - Documenting of the processes and procedures.
  - Management approval.

GUIDELINES

When applying software patches, agencies should consider that:

- Ignored and unpatched software vulnerabilities can represent a great risk to the security of State information assets.
- They should have and implement a procedure for identifying and applying patches that address security vulnerabilities.
- Patch application is no different than introducing a new or updated program into the system and carries the same potential for damage and system compromise.
- Applying a patch or upgrade requires the same strict control as any other system change.

- Whenever a patch is implemented, the application systems it affects should be tested to ensure that business operations and security controls perform as expected.
- Appropriate updates should be made to both system documentation and business continuity plans.

ISO 17799: 2005 REFERENCE
12.5.1 Change control procedures

040202 Upgrading Software

Purpose: To protect against the security risks associated with software upgrades

STANDARD

Software upgrades shall not be installed in a production environment (mainframes, servers and desktop computers) until the following conditions are met:

- Qualified personnel certify that the upgrade has passed acceptance testing and demonstrate the following:
  - ❑ System security controls remain effective.
  - ❑ Computer capacity and performance requirements are not adversely affected.
  - ❑ System documentation and business continuity plans are amended to reflect upgrade.
  - ❑ A rollback plan has been developed in the event the upgrade has unacceptable ramifications.
- Management has agreed that the desired acceptance criteria has been met.

GUIDELINES

Agencies should remember that software upgrades may have impacts on other systems. The change control process should not be classified as complete until team members can verify the following:

- There are not any additional risks imposed on information security throughout the agency's environment.
- There are not any interdependent systems that have had loss of functionality due to the upgraded software.

RELATED INFORMATION

Standard 040105	Implementing New/Upgraded Software
Standard 140102	Assessing the Business Continuity Plan Security Risk

ISO 17799: 2005 REFERENCES
10.3.2 System acceptance
12.5.1 Change control procedures

040203 Responding to Vendor Recommended Upgrades to Software

Purpose: To mitigate the risks associated with applying vendor-recommended software upgrades

STANDARD

Agencies shall implement vendor-recommended upgrades for use in a production environment only after the following conditions are met:

- Security is not compromised by any upgrade and security controls are in place.
- There is a business justification that warrants software upgrades.
- Qualified agency staff validate the technical need for a vendor-recommended upgrade.

GUIDELINES

Agencies should consider the potential impact that vendor-recommended upgrades may have on the following:

- The potential for information security vulnerabilities inherent in new or upgraded software.
- Increased technical requirements and costs associated with a software upgrade.
- The balance between the need to continue current operations and the understanding that certain levels of software currency must be maintained to receive continued vendor support for the software.
- The possibility that systems that rely on functionality provided by the system that is being upgraded may prove to be incompatible with the upgrade.
- Additional training necessary for business and technical users to cover new features and security controls introduced by the upgrade.

RELATED INFORMATION

Standard 040101	Specifying User Requirements for Software
Standard 140102	Assessing the Business Continuity Plan Security Risk

ISO 17799: 2005 REFERENCES
10.3.2 System acceptance
12.5.1 Change control procedures

040204 Interfacing Applications Software / Systems

Purpose: To mitigate risks associated with linking various application software programs or systems together.

STANDARD

Agencies that develop interfacing systems shall ensure that the interfacing systems integrate appropriate security to ensure the confidentiality, as applicable, and the integrity and availability of data. When implementing interfacing applications software/systems, due-diligence measures shall include, but shall not be limited to, the following:

- Implementing recommended security controls.
- Utilizing risk management practices to align the business value of the information assets (e.g., database programs to Web applications) being integrated and the potential loss or damage that might result from a security failure.
- Meeting with developers to determine whether data will need to be reformatted or otherwise modified to meet the needs of the interfacing system.
- Ensuring that software development procedures begin with planning and have adequate process and management controls.
- Utilizing qualified software development staff experienced in interfacing systems.

GUIDELINES

Agencies should consider the following information security issues when analyzing or justifying interfacing system projects:

- Developing interfacing systems is a technical task that is accompanied by high risks.
- Application security is more efficient and more cost effective when implemented at the beginning of a project.
- Prior permission should be secured for the reading of databases not normally under the control of the application that will read them.
- Interfacing applications software/systems should be designed so that levels of authority among the applications or systems are clearly defined to protect the integrity of the data residing on the interfaced application/system.

ISO 17799: 2005 REFERENCES
12.1.1 Security requirements analysis and specification
12.2.1 Input data validation
12.5.2 Technical review of operating system changes

040205 Supporting Application Software

Purpose: To protect application software by providing adequate technical support

STANDARD

Agencies shall provide adequate levels of technical support necessary to support business processes. Levels of technical support shall require that:

- Security measures be used to mitigate risks and security vulnerabilities.
- Software issues be handled efficiently.
- Software problems be resolved in a timely fashion.

GUIDELINES

If one is available, an agency's primary avenue for user software support should be a help desk. The help desk should have formal software problem resolution procedures that promote the following best practices:

- Tracking problems from initial reporting through to resolution.
- Monitoring status of reported problems and confirming that satisfactory resolutions have been achieved.
- Providing reports and metrics for system development and software support management (i.e., for trend analysis, lessons learned, etc.)
- Maintaining a pool of software technicians with the appropriate skill sets to assist with software problem resolution.
- Building a database of institutional knowledge that reflects trends, common problems, etc., and sharing it with other State agencies.

ISO 17799: 2005 REFERENCES
6.2.3 Addressing security in third party agreements
12.1 Security requirements of information systems
12.5 Security in development and support processes

040206 Operating System Software Upgrades

Purpose: To mitigate risks associated with upgrading operating systems.

STANDARD

Operating system (OS) upgrades shall be carefully planned, executed and documented as a project. Agencies involved in operating system software upgrades to systems shall perform the following steps before commencement of the upgrade project:

- Document that system security controls will remain effective or will be modified to appropriately respond to the OS upgrade.
- Locate change control processes and procedures.
- Document agreement of technical staff and management to acceptance criteria.
- Document that qualified personnel have certified the upgrade and that it has passed user acceptance testing.
- Establish a rollback plan in the event the upgrade has unacceptable ramifications.

GUIDELINES

Agencies should consider the following security issues when upgrading an OS:

- An OS failure can have a cascading adverse effect on other systems and perhaps even the network.
- System documentation and business continuity plans should be amended to reflect the OS upgrade.
- Since OS upgrades typically affect many systems within an agency, such upgrades should be part of the annual maintenance plan/budget. OS upgrade testing and review cycles should also be included in this budget.

RELATED INFORMATION

Standard 140102	Assessing the Business Continuity Plan Security Risk
Standard 040106	Technical Vulnerability Management

ISO 17799: 2005 REFERENCE
12.5.2 Technical review of applications after operating system changes

040207 Support for Operating Systems

Purpose: To provide maximum availability, security and stability of operating systems.

STANDARD

Each agency shall ensure that the operating systems used to run the production environment are regularly monitored for security risks and maintained in approved secure configurations to support business operations.

GUIDELINES

Agencies should consider the following issues when supporting operating systems:

- New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities.
- Operating systems performance is benefited by periodic maintenance (e.g., hard drive defragmentation).
- The operating systems on servers, minicomputers and mainframes usually require daily maintenance tasks and routines that:
  - May be initiated manually as a result of an alert or logged event.
  - May be scripted to run automatically when a certain threshold or limit is exceeded.
- Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure that:
  - Maintenance tasks continue to perform as expected.
  - Operating systems continue to operate within accepted thresholds.
  - System security is not being compromised by maintenance tasks.

- Maintenance tasks do not adversely affect computer capacity or performance.

ISO 17799: 2005 REFERENCES
12.5.2 Technical review of applications after operating system changes

040208 Recording and Reporting Software Faults

Purpose: To identify and correct software faults efficiently and effectively.

STANDARD

Each agency shall ensure that software faults or bugs are formally recorded and reported to those responsible for software support and maintenance.

Software faults that pose a security risk shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability.

Agencies shall include the following security issues when establishing or reviewing software support procedures:

- Software fault-reporting procedures shall be taught and encouraged through security training and awareness programs.
- Agencies shall designate a quality control team that consistently checks for faults and that is responsible for reporting them to software support.
- Agencies shall use a formal recording system that:
  - Tracks faults from initial reporting through to resolution.
  - Monitors the status of reported faults and confirms that satisfactory resolutions have been achieved.
  - Provides reports and metrics for system development and software support management.

While faults are being tracked through to resolution, research shall also be conducted to ensure that:

- No IT security controls have been compromised.
- Resolution activities have been appropriately authorized.

ISO 17799: 2005 REFERENCES
10.10.5 Fault logging

Section 3 Other Software Issues

040301 Disposing of Software

Purpose: To protect information by using secure software disposal techniques.

STANDARD

Software removal and disposal may be initiated only after a formal decision to stop using the software has been made by senior management and steps have been taken to protect the information contained in the software application.

Before disposal of software, agencies shall protect information developed using the software by:

- Following orderly termination procedures to avoid disruption of business operations.
- Migrating data to another system or archiving data in accordance with applicable records management regulations and policies for potential future access.
- Using a State-approved technique to ensure that no data remain on the media (e.g., by incineration, shredding, degaussing or sanitizing of data for use by another application within the organization).
- Logging the disposal of media containing confidential information to maintain an audit trail.

GUIDELINES

Agencies should consider the following information security issues and controls when involved in software disposal:

- Emphasis should be given to the proper preservation of the data processed by the system so that:
  - Sufficient vital information about the system is preserved so that some or all of the system may be reactivated in the future.
  - The backup strategy that is utilized is able to recover the actual program and program files to enable retrieval or access of data stored in the application.
- Software media storage and disposal should follow industry best practices and vendor and manufacturer specifications.

ISO 17799: 2005 REFERENCES
10.7.2 Disposal of media

HISTORY

Approved by State CIO: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
Permanent Removal of Data from Electronic Media Standard	040301 – Disposing of Software
	030903 – Using External Disposal Firms
	050701 – Disposing of Obsolete Equipment
Vulnerability Management Standard	040106 – Technical Vulnerability Management